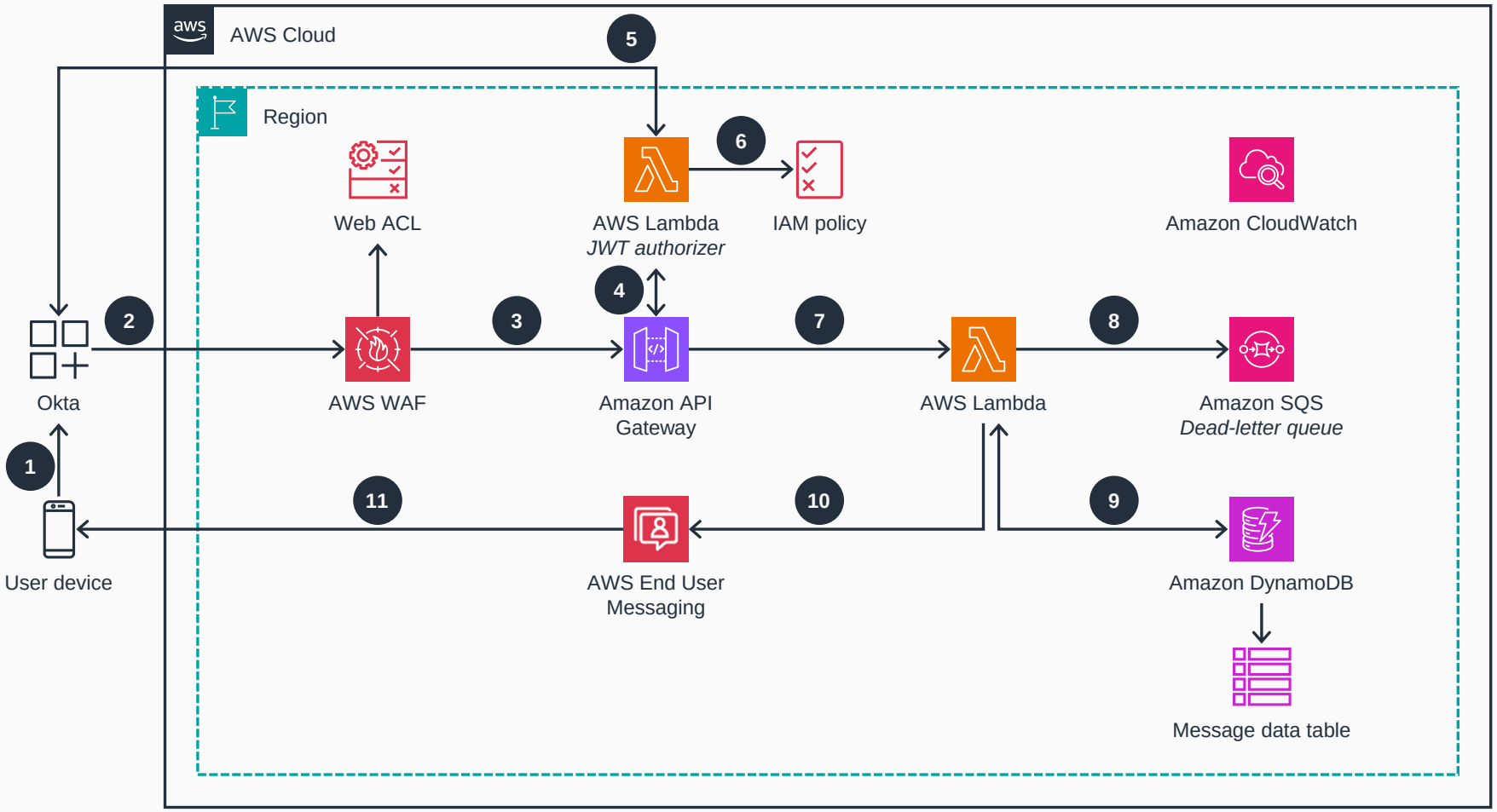
Guidance for Okta Phone-Based Multi-Factor Authentication on AWS

This architecture diagram shows how to integrate Okta's telephony inline hook with AWS services to implement a secure and scalable solution that delivers OTPs using SMS or voice calls. This slide details steps 1-8.



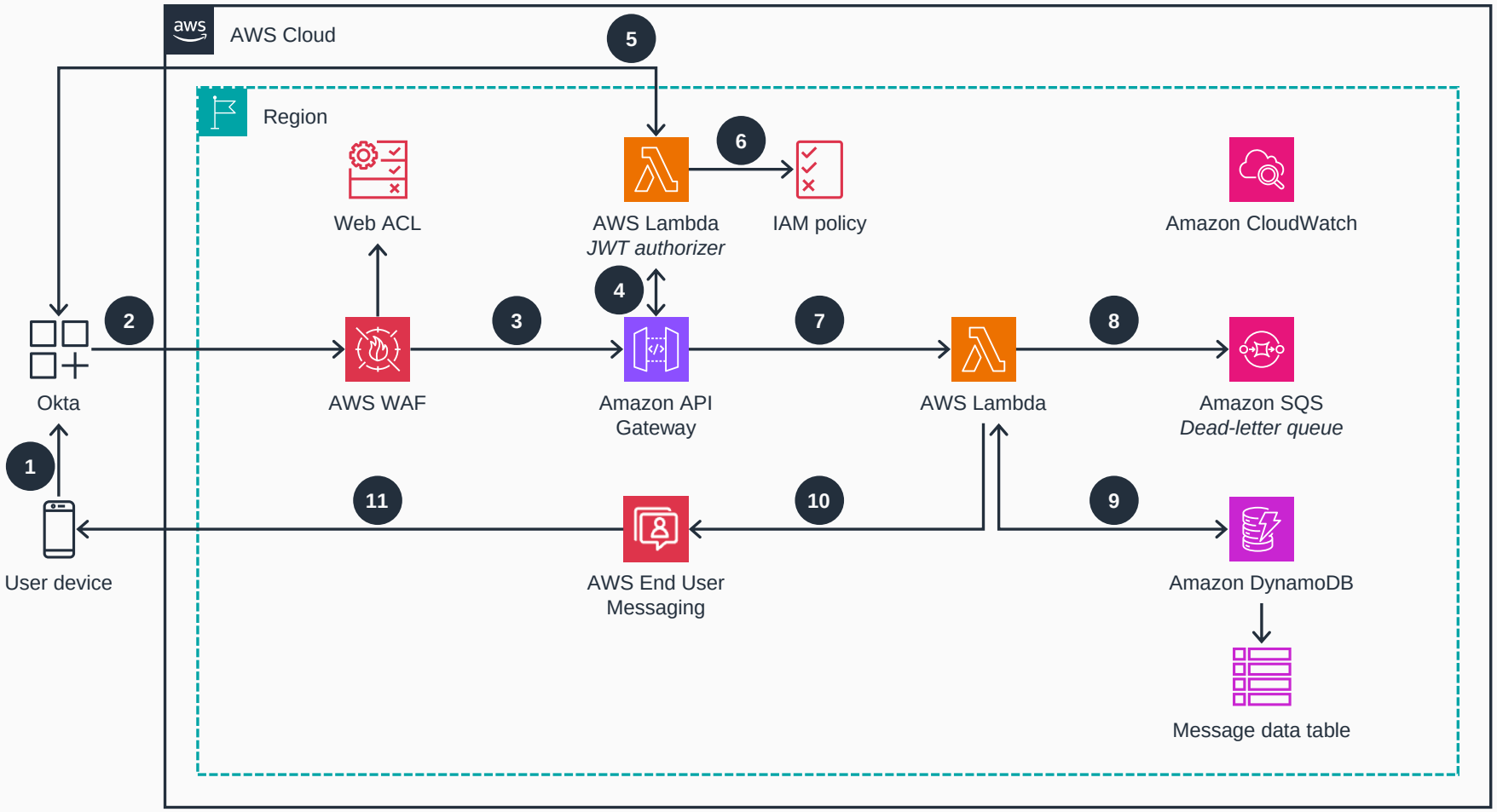
1. A user initiates sign-in on Okta and is prompted for phone-based authentication. The user chooses SMS or voice delivery to receive the OTP. Okta's telephony inline hook is activated, creating a JSON web token (JWT) request for OTP delivery through **Amazon API Gateway**.
2. **AWS WAF** protects the **API Gateway** endpoint by applying rules managed by AWS to block malicious traffic. All traffic is filtered through **AWS WAF** web access control lists (ACL), and requests deemed safe are allowed to pass through to **API Gateway**.
3. **API Gateway** first receives the JWT request from Okta. It then invokes a custom **AWS Lambda** function that acts as an authorizer to validate the JWT token before allowing the request to proceed.
4. The **Lambda** authorizer is responsible for verifying the integrity and validity of the JWT token. It performs several checks to ensure the token is valid.
5. The **Lambda** authorizer verifies the JWT token by decoding it, using Okta's public key to validate the signature and checking the expiration time.
6. If the JWT token is valid, the **Lambda** authorizer creates an **AWS Identity and Access Management (IAM)** policy that grants permission to invoke **API Gateway**.
7. The **Lambda** authorizer returns the **IAM** policy to **API Gateway**. If access is allowed, **API Gateway** is invoked and forwards the request to the backend **Lambda** function.
8. If the **Lambda** function encounters an error or exception while processing the user's request, it may send the request to an **Amazon Simple Queue Service (Amazon SQS)** dead-letter queue for further investigation and troubleshooting.

Reviewed for technical accuracy September 25, 2024

AWS Reference Architecture

Guidance for Okta Phone-Based Multi-Factor Authentication on AWS

This architecture diagram shows how to integrate Okta's telephony inline hook with AWS services to implement a secure and scalable solution that delivers OTPs using SMS or voice calls. This slide details steps 9-11.



9 If no errors are found, the **Lambda** function contacts **Amazon DynamoDB** to retrieve message data based on the user's request details, such as their language preference and their choice of SMS or voice delivery. A **DynamoDB** table stores message templates tailored for various languages and communication methods. The **Lambda** function retrieves the appropriate message template that matches the user's request details.

10 The **Lambda** function retrieves the message data and uses it to create a personalized message for the user. The message includes the OTP authentication code. Depending on the user's chosen method of communication, the function formats the message accordingly.

11 **AWS End User Messaging** then sends the message to the user. For SMS, it sends a text message directly to the user's phone. For voice delivery, it converts the text into a voice message and delivers by phone call.

Reviewed for technical accuracy September 25, 2024

AWS Reference Architecture